

[illegible]

## 5

10

15

25

1

If a building cleaning service has to clean and care for certain parts of the building at certain times, the cleaning personnel must be given corresponding rights of entry. This is generally done by handing to the cleaning personnel one or more mechanical keys which are not able to unlock certain doors. When this is done, there is  
5 no guarantee that the person who has possession of this key is also a member of the cleaning personnel. There is a further problem in that if the key is lost, substantial damage can occur. In this situation misuse cannot be ruled out.

If a resident of the building expects several guests, he must provide each individual visitor who reports to reception with access to the building and if necessary,  
10 each time anew give a description of the way to find him in the building. Under certain circumstances this can be quite tedious.

If in the building or in an apartment of the building a one-time or rarely repeating service is performed, authorization of access for the service personnel can only be arranged with high administrative outlay. Either a person must accompany the service  
15 personnel, or a mechanical key must be made available for the service personnel, which requires a certain amount of trust in advance and increases the danger of misuse.

### SUMMARY OF THE INVENTION

An objective of the present invention is therefore to specify a method of initiating  
20 a procedure within a building by means of which certain components of the infrastructure of the building can be automatically and faultlessly made available to an authorized person in a safe manner. With the method according to the present invention for initiating a procedure in a building, a virtual key is generated by a certain event. The virtual key is then communicated to a person. If the authorized person identifies himself  
25 by means of the key, the procedure is initiated in the building.

It is advantageous for the key to be assigned a certain code by means of an encryption method.

Furthermore, it is an advantage to add to the key a signature with which the recipient of the key can identify himself to third parties as the person authorized to use it.

30 It is also an advantage for the type of procedure to be made dependent on the type of event.

It is advantageous for the procedure to control an elevator situated in a building.

Another advantageous further development of the present invention is that the person to whom the key is communicated is made to depend on the type of event.

Moreover, it can be checked whether for the person to whom the key is communicated a key already exists and if so, whether it is being used with modification.

5 A further advantage of the invention is that the means which the person to be authorized has available to identify himself are ascertained, and a suitable one of them is selected.

In a further embodiment of the invention, if a key already exists, it is checked whether this fulfils the security requirements and if necessary, a new or augmented key is  
10 generated.

It is advantageous for the person to identify himself when receiving the key.

#### DESCRIPTION OF THE DRAWINGS

The above, as well as other advantages of the present invention, will become  
15 readily apparent to those skilled in the art from the following detailed description of a preferred embodiment when considered in the light of the accompanying drawings in which:

Fig. 1 is a flowchart for the method according to the present invention of initiating a security procedure within a building.

20

#### DESCRIPTION OF THE PREFERRED EMBODIMENT

As shown in Fig. 1, the initiating element is a certain event identified as a starting point "Event" 11. As already mentioned above, the event can be an emergency call, an order, a request such as for a cleaning service, an invitation, or a periodically recurring  
25 event such as, for example, monitoring a condition, or a service.

The type of event determines what requirements are specified for a key that is to be generated. For example, if a fire occurs in the building, the requirements for the security of the key must be set less high and the requirements for the availability of the key must be set higher. If, however, the initiating event is giving to a cleaning service  
30 the task of cleaning the building, the security requirements for the key to be issued must be set significantly higher. This means that in this case, the danger of misusing the key must be kept as low as possible, whereas in case of fire, access to the building must be

guaranteed under all circumstances. In consequence, different types of events place different requirements on the key to be issued in a processing step "Specify Requirements for the Key" 12.

The term key or virtual key as used herein is to be understood as a code.

5 It is also through the event that the person to be authorized is defined. If, for example, the initiating event is an emergency call, for this event the emergency physician must be called, whereas if the initiating event is a personal invitation of a resident of the building, the guest or guests must be invited. The person is defined in a processing step "Specify Person to be Authorized" 13.

10 Whether the requirements for the key are defined first, and then those for the persons(s) to be authorized, depends on the circumstances describing the system. Thus, the order of steps 12 and 13 can be reversed.

After this, it must be ascertained whether means are available from the person to be authorized which can be used as a key. Examples of possible means are  
15 communication means such as a telephone, mobile radio, pager, or PC. The means are ascertained in a step "Ascertain Whether Means are Available from the Person to be Authorized Which Could Serve as a Key" 14.

Examples of possible means for a key are a secret word, a secret number, a sentence, a symbol, or a picture.

20 After the requirements for the key have been defined, and the person who is to be authorized has been defined, and it has been ascertained whether means are available from the person to be authorized which can be used as the key, it is checked whether the quality of a key which may be present fulfils the requirements at a decision point "Quality OK?" 15. If this is not the case, the method branches at "No" to a processing  
25 step 16 wherein a new key is generated, or else the key which is present is augmented to the extent necessary to fulfil the requirements for the key.

After a suitable key has been generated, or the initial quality of the key was acceptable, the method branches from the step 15 at "Yes" to a processing step "Transmit Key" 17 where the key is communicated to the authorized person. The type of  
30 transmission depends on the means available to the authorized person. If the authorized person has a mobile radio telephone, the transmission can take place over an interface of air. However, if the key must be transmitted to a fax device, wired transmission is

generally used. The type of communication of the key depends on the technical circumstances.

If necessary, identification of the authorized person can already take place when the key is received. This can be done, for example, with biometric characteristics such as the voice of the recipient, or his fingerprint. After the key has been received in a method step "Receive Key" 18 and, if necessary, the person authorized to use it has identified himself, the key is stored in a method step "Store Key" 19 on the means of transmission available to the authorized person. However, this is not absolutely essential. The person authorized to use the key can remember it himself.

As soon as the person authorized to use the key arrives at the respective building, the key comes into use in a method step 20. Depending on the key, use of the key takes place by entering the secret number, the secret word, or similar on a keyboard, or detection of the key in spoken form by a microphone on the building, or the biometrics features of the person authorized to use the key by a corresponding biometrics sensor arranged on the building.

After the key has been entered, a check is made of the key for validity at a decision point "Key Valid?" 21. If the key is recognized to be invalid, for example if the key can only be used for a specified period of time and is used later than this, it is rejected by branching at "No" and terminating the process at an end point "End" 22. The person does not obtain access to the building, the procedure is not initiated.

On the other hand, if the key is recognized as valid, the process branches at "Yes" to a process step "Initiate Procedure" 23 wherein the procedure is initiated, for example the doors of the building are opened, the elevator is made available, the elevator doors opened, and any security barriers which may be present are released. A further procedure can be transmission of a message to the sender of the key. Further, the user of the key can be given information about the way to get to the person who sent the key. A greeting to the person authorized to use the key, or other items of information left for the authorized user, can now be delivered. The initiated procedure can also include an automatic trip of the elevator to the destination floor. Finally, the procedure can also be a receipt for delivery of the goods or service. Upon completion of the procedure, the process terminates at an end point "End" 24.

By means of the method according to the present invention, an electronic key for granting access to certain areas as a result of external events, for example an order by mail, a request for help, detection of fire, and so on is automatically generated and delivered. This means that the initiating event automatically implies the requirement for  
5 access, and that the necessary steps (provision and dispatching of the key) are taken. For example, a request for an emergency physician by means of an emergency transmitter causes a code to be delivered to the physician. With this, the physician identifies himself to the access control system, so as to be able to reach the patient unhindered.

The electronic key can, for example, be implemented in the form of a binarily  
10 represented number or sequence of numbers. The relevant persons involved in generating the key, and in distributing and using the key, are the ordering person (for example the person to be visited), the visitor, and an administrator. When doing so, various forms and methods of identification and authentication are possible such as those provided by public key cryptography. In this connection, reference should be made to  
15 the publication of R. L. Rivest, A. Shamir, and L. Adleman "A Method for Obtaining Digital Signatures and Public-key Cryptosystems", 1977. In that work, a coding method is described with which an encryption key is publicly accessible without the decryption key being made publicly accessible. The method is also known as the RSA method.

In a simple embodiment of the key, the key can be augmented with a PIN code,  
20 an identifier, a telephone number, or a secret word. Greater protection against misuse can be obtained by using a public key as authentication, and corresponding encryption methods for communication. When doing so, in a first phase public keys based on authentication are used. If a user is to be granted access or other rights, he receives these rights securely sent to him in numerical form and by means of the public key. When  
25 using the rights, decryption takes place which ensures that the declared rights as, for example, of access are granted by an authorized source. Furthermore, a method of signing can be added which enables corresponding proof to third parties.

The key can contain various items of information. It is possible that a part of the key is a signature of the recipient or the administrator. A further part of the key can be  
30 the initiating event itself. It is even possible to add items of information to the key which contain, for example, the access rights, i.e. who may have access to where, and when. Further, the type of right can be documented in the key. Finally, it is also possible to

store in the key only a reference or a pointer that indicates the address in storage under which the administrator has stored the additional information.

Depending on the specific application, the key can be stored completely or partially in one or more places. If the key is stored completely in several places this  
5 means high redundancy and therefore high certainty of access, but also a high danger of misuse. Storing the key in its complete form in several places can be helpful, for example in case of fire in the building.

The items of information stored in the key can be transmitted to the building's own receiver via, for example, an infrared interface (IRDA) or a Bluetooth radio  
10 interface of a mobile radio telephone.

IRDA (Infrared Data Association) defines an infrared communication standard. It can be used to create wireless connections with a range of between 0 and 1 meter and a data transmission rate of between 9600 and 16 Mbaud.

Bluetooth is intended for short-range voice and data traffic at radio frequencies of  
15 2.4 GHz in the ISM band. Its range lies between 10 cm and 10 m but can be extended up to 100 m by increasing the transmission power.

Generation and distribution of the key can also be performed by different sources such as, for example, an alarm trigger, the building administrator, or a third source. Generation of the key is automatically based on an indication such as that given by  
20 triggering of an alarm.

With receipt of the key, other items of information and instructions can be transmitted such as, for example, a sketch showing the way, a restriction on visiting times, or operating instructions.

When the key is used it is possible, for example, for the purpose of informing or  
25 authenticating the user, to create a communication connection between the key transmitter and the key bearer.

Furthermore, it is possible to inform the sender of the key if the key has not been used after expiry of a certain period of time. It is also possible to modify the rights granted to the authorized user, so that the authorized user is no longer authorized to use  
30 the key, or only with limitations. As well as this, the rights of all keys can be modified. This can be of significance if a number of keys have been distributed, but from now on only some of them may be used.

The sender of the key or the administrator can be notified if the key functions incorrectly and/or there are attempts at manipulation.

The key can be embedded in a higher-level program so that, for example, an operating program can be transmitted together with the key to a mobile telephone with  
5 WAP browser. The telephone can then be used as an operating interface inter alia to make use of the key.

Furthermore, it is possible to charge a fee for each use of the key which can depend on the type of key and the action or procedure which is initiated. Charging can be to the key owner, in other words the authorized user, the sender of the key, or  
10 someone else.

As well as this, it is possible to use the key to switch to a special operating mode when the key is used. This could be especially important for the fire service in case of fire, so they can control an elevator.

If a key is used, this can be indicated visually and/or acoustically.

15 If a key is not used, this can cause certain actions to be initiated, such as a reminder message to the recipient of the key.

Further, when the key is used, additional information can be transmitted to the lock, in other words the electronic recipient. The type of information can then be determined by the key itself and/or requested by the lock. The information can contain,  
20 for example, details of the visitor such as personnel number, preferred room temperature, or ability to communicate.

In accordance with the provisions of the patent statutes, the present invention has been described in what is considered to represent its preferred embodiment. However, it should be noted that the invention can be practiced otherwise than as specifically illustrated  
25 and described without departing from its spirit or scope.